SMtools User Manual

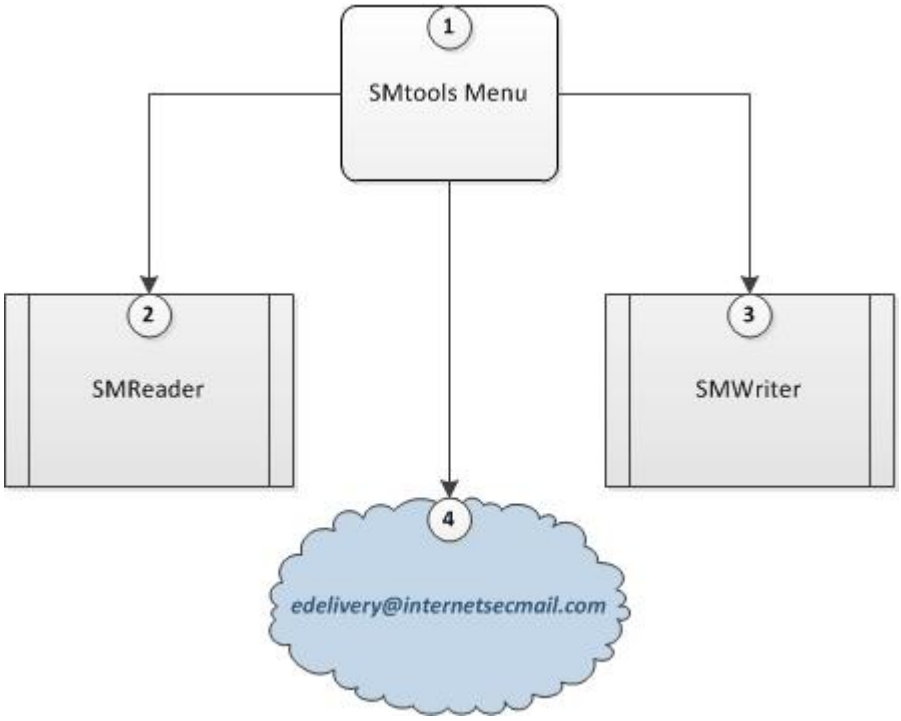
Table of Contents

SMtools –InternetSecMail Desktop Encryption/Decryption tools 2
Key Management Commands 5
createkeys 5
recreatekeys 5
Sync commands 5
Show Key Commands 5
Lockmembers {MemberName1,MemberName2…} 5
SMreader Interface Commands 6
whatsin 6
decrypt {InputFile PasswordFile} 6
archivein {ArchiveName} 6
SMwriter Interface Commands 7
whatsout 7
whatshout members 7
whatsout outbox 7
preparearchive 7
SMmenu general notes 10

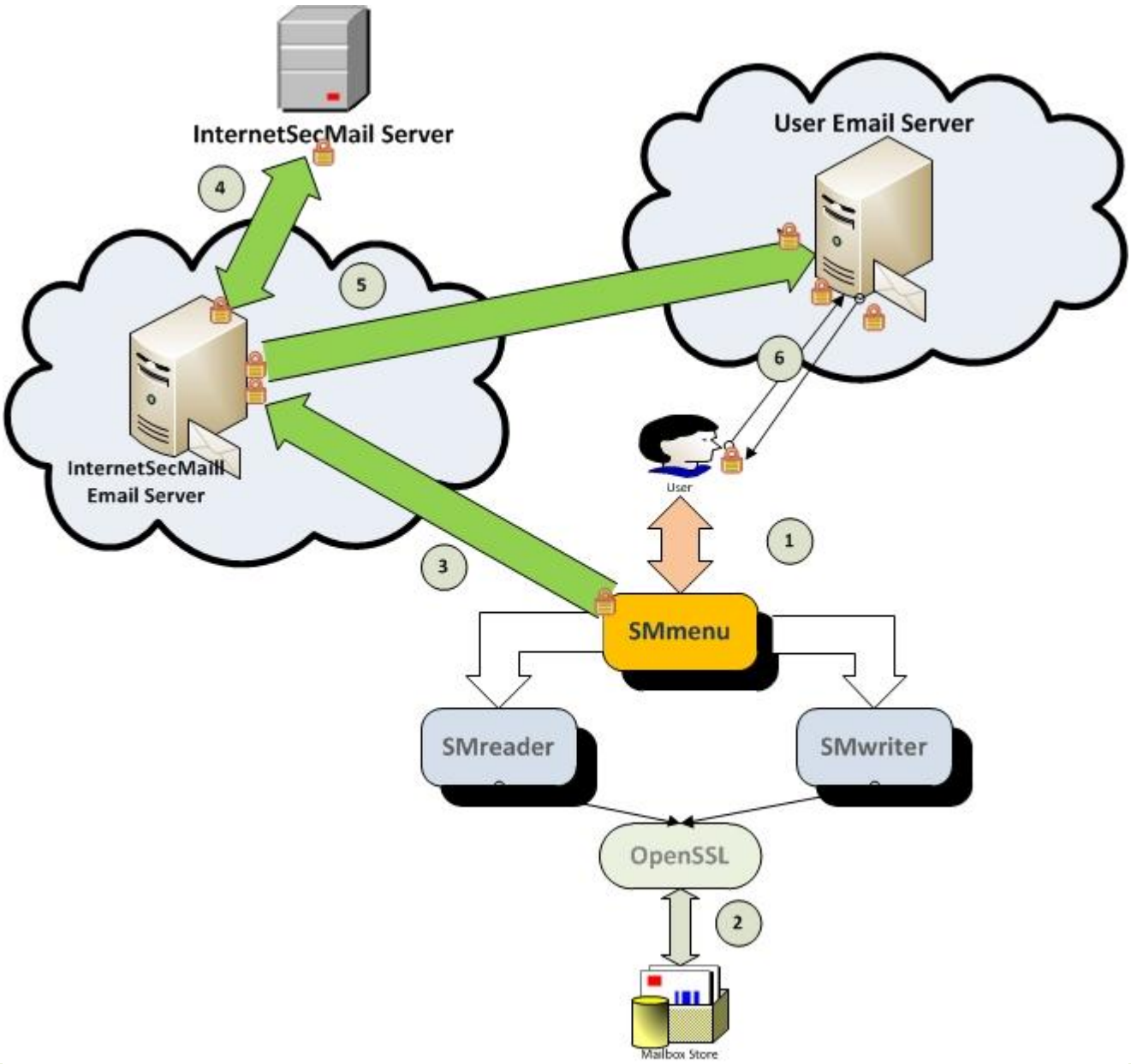
SMtools –InternetSecMail Desktop Encryption/Decryption tools

In order to provide **InternetSecMail** members ability to communicate with maximum privacy and confidentiality, **InternetSecMail** offers simple command line interface for Desktop **CYGWIN** environment called **SMtools**.
SMtools containg **SMmenu** – high level **Menu Interface** activated from CYGWIN terminal.
The **SMmenu** relays on 2 basic utilities **SMwriter** and **SMreader** which communicate with **OpenSSL** to provide encryption/decryption services.

Using **SMtools**, the **InternetSecMail Members** can communicate with each other securely, while the encryption and decryption of the messages is implemented completely on the **User Desktop** and the **InternetSecMail** server is used as a **Message/Key Repository intermediary Server**:

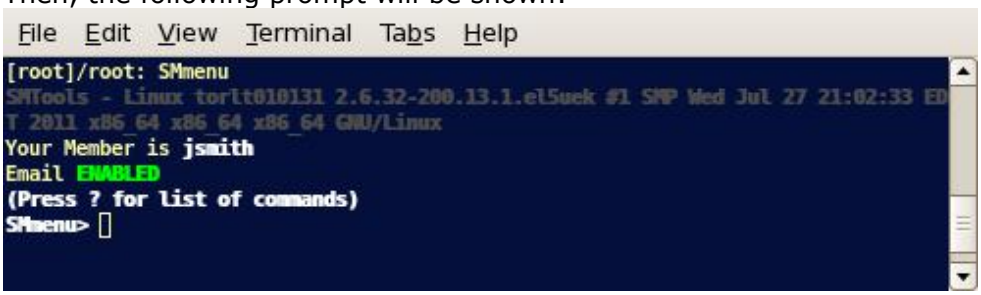


The next diagram explains the architecture of **SMtools** in more details:

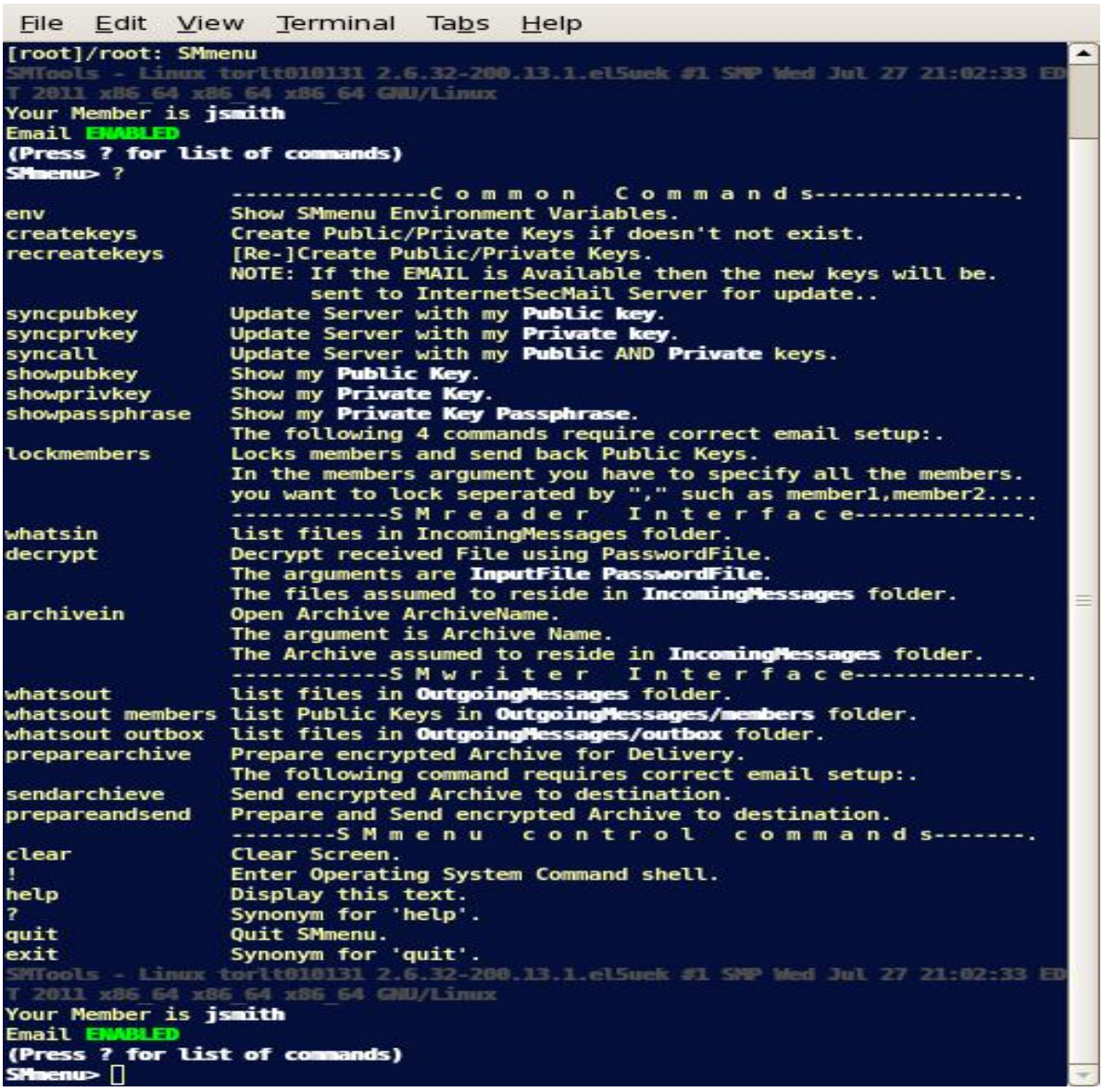


1. The User communicates with **SMmenu**. The **SMmenu** provides following functionality:
   - Keys Management Services (will be explained in special section)
   - Decrypt incoming messages.
   - Encrypt (and send) outgoing messages.
2. The **SMreader** and **SMwriter** utilities are called by **SMmenu**. Those tools communicate with low level **OpenSSL** functionality for all related functions (encrypt, decrypt, prepare Keys, sign, verify signatures).
3. If the **SMmenu** needs to send request to **InternetSecMail Server**, it uses User Configured SMTP communication channel. User can define this channel as SSL/TLS protected (S/MIME) if his Email Provider allows such kind of communication.
4. The **InternetSecMail** scans incoming box (edelivery@internetsecmail.com) using SSL protected channel for the new requests.
5. After request been processed, the results are sent using SSL protected channel from output mailbox (member@internetsecmail.com) to the *Primary Email Address* of the User.
6. The User receives the answers from InternetSecMail in his **private Mailbox** (*Primary Email Address*).

To activate SMmenu, the user has to open his CYGWIN terminal (X-Terminal in UNIX/LINUX) and to type SMmenu.
Then, the following prompt will be shown:


File Edit View Terminal Tabs Help
[root]/root: SMmenu
SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 EDT 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu>

The "?" command displays the list of available commands as shown:


File Edit View Terminal Tabs Help
[root]/root: SMmenu
SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 EDT 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu> ?
----------Common Commands----------
env Show SMmenu Environment Variables.
createkeys Create Public/Private Keys if doesn't not exist.
recreatekeys [Re-]Create Public/Private Keys.
NOTE: If the EMAIL is Available then the new keys will be.
sent to InternetSecMail Server for update..
syncpubkey Update Server with my Public key.
syncprvkey Update Server with my Private key.
syncall Update Server with my Public AND Private keys.
showpubkey Show my Public Key.
showprivkey Show my Private Key.
showpassphrase Show my Private Key Passphrase.
The following 4 commands require correct email setup:.
lockmembers Locks members and send back Public Keys.
In the members argument you have to specify all the members.
you want to lock seperated by "," such as member1,member2....
----------SMreader Interface----------
whatsin list files in IncomingMessages folder.
decrypt Decrypt received File using PasswordFile.
The arguments are InputFile PasswordFile.
The files assumed to reside in IncomingMessages folder.
archivein Open Archive ArchiveName.
The argument is Archive Name.
The Archive assumed to reside in IncomingMessages folder.
----------SMwriter Interface----------
whatsout list files in OutgoingMessages folder.
whatsout members list Public Keys in OutgoingMessages/members folder.
whatsout outbox list files in OutgoingMessages/outbox folder.
preparearchive Prepare encrypted Archive for Delivery.
The following command requires correct email setup:.
sendarchieve Send encrypted Archive to destination.
prepareandsend Prepare and Send encrypted Archive to destination.
--------SMmenu control commands--------
clear Clear Screen.
! Enter Operating System Command shell.
help Display this text.
? Synonym for 'help'.
quit Quit SMmenu.
exit Synonym for 'quit'.
SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 EDT 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu>

The first command env shows the **SMtools** Environment Variables as they defined during the Installation Process (See **SMtools** Installation Manual for details).
The rest of commands in this section (Common Commands) are dealing with various Key Management aspects as explained in the next section:

Key Management Commands

createkeys

The **createkeys** command creates Public/Private Keys pair in user directory pointed by **$SM_KEYDIR** environment variable. The Private Key is protected by randomly generated 12 characters long *passphrase* stored in location pointed by **$SM_PASSPHRASE** environment variable.
If the Public/Private Key files already exist, the command has no action.
If the *passphrase* file already exists, the command uses the *passphrase* from existent file.

recreatekeys

The **recreatekeys** command overwrites existent Public/Private key files with new values.

Note: It is highly recommended to update the Keys in internetSecMail Keys Repository either from Web Interface or by **sync** commands as soon as they changed in your Private Environment.

Sync commands

syncpubkey, **syncprvkey**, **syncall** commands sends your Public, Private or ALL keys to **InternetSecMail** Server for synchronization with central repository.
Note that your *passphrase* is NOT sent to InternetSecMail Server in any way. The InternetSecMail also never stores your *passphrase* even if the *passphrase* is generated by InternetSecMail Web Interface.
You have to protect your *passphrase* in the way which is most convenient for you and not to disclose it to person. Without the passphrase you will not be able to decrypt the encrypted incoming messages, even if your Private Key has been disclosed.

Show Key Commands

The **showpubkey**, **showprivkey** and **showpassphrase** show the content of your Key Files or your passphrase.

lockmembers **{MemberName1,MemberName2…}**

The **lockmembers** command send request to **InternetSecMail** to lock the **Public Keys** of the specified **Members**. The purpose of this command is to prevent changing of Public Key by Member while you prepare the confidential message to this Member using his current Public Key.
This operation is equivalent to **Lock Member** from **Contacts Management** Web Interface screen. Save the received **Key Files** into **$SM_OUTDIR/members** folder.

SMreader Interface Commands

The **SMreader** interface commands provide the wrapper to **SMreader** tool. Although you can use **SMreader** tool from command line, it's easier to have the Single point of Control provided by **SMmenu**.

whatsin

The **whatsin** command shows files in the directory pointed by **$SM_INDIR** Environment Variable.
When you receive the emails from different Members, the content arrives into your mailbox as encrypted attachments. The **$SM_INDIR** location defines unique target location for all encrypted attachments you receive from other members and save them using "save as" command.

decrypt {InputFile PasswordFile}

When you receive encrypted emails from other Members, the emails can be prepared in 2 ways:

1. Sending encrypted email using InternetSecMail Web Interface
2. Sending encrypted email using SMtools.

If the email contains attachments the other member sent using **InternetSecMail Web Interface**, the attachments will contain following files:

a. The **Password File** contains decryption password for **Data Files**. This **Password File** is encrypted by your **Public Key**.
b. The **Data Files** encrypted by password that should be extracted from **Password File**.

The command **decrypt** calls **SMreader** by supplying Input **Data File** and **Password File** as a parameters.

archivein {ArchiveName}

When the Member sends encrypted email using SMtools, the attachment file comes as self-contained Archive having special format (see **prepparearchive** command for more details). The **archivein** command forces SMreader to open the Archive using following steps:

1. Open and extract the Archive into target directory (named same as Archive).
2. Decrypts the Password File using your Private Key (and *passphrase*).
3. Decrypts each Data File found in Archive by the password extracted from Password File.
4. Check signature for each decrypted Data File to verify that they are coming from the claimed Member.

SMwriter Interface Commands

The **SMwriter** interface commands provide the wrapper to **SMwriter** tool. Although you can use **SMwriter** tool from command line, it's easier to have the Single point of Control provided by **SMmenu**. In addition, **SMmenu** allows you to utilize additional options which are not available from **SMwriter** tool.

whatsout

The **whatsout** command shows the content of location pointed by **$SM_OUTDIR** Environment Variable. The following commands **preparearchive**, **sendarchive** and **prepareandsend** using this directory as Top level location for subsequent folders.

whatshout members

The **whatsout members** command shows Public Keys of the Members you can send emails to. The **members** is a sub directory under **$SM_OUTDIR**.

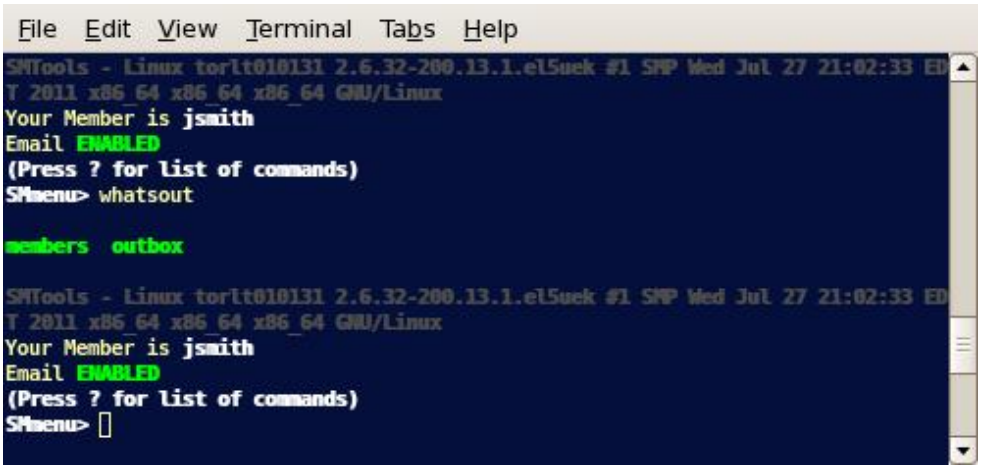
whatsout outbox

The **whatsout outbox** command shows the content of outbox – the location where you store all your messages and attachments you want to encrypt and sent to target Member. Note, that the ***Member Key*** must be present in **members** folder prior using **preparearchive**, **sendarchive** and **prepareandsend commands.** To obtain Member's Public Keys, use **lockmembers** command and save the received **Key Files** into **members** folder.

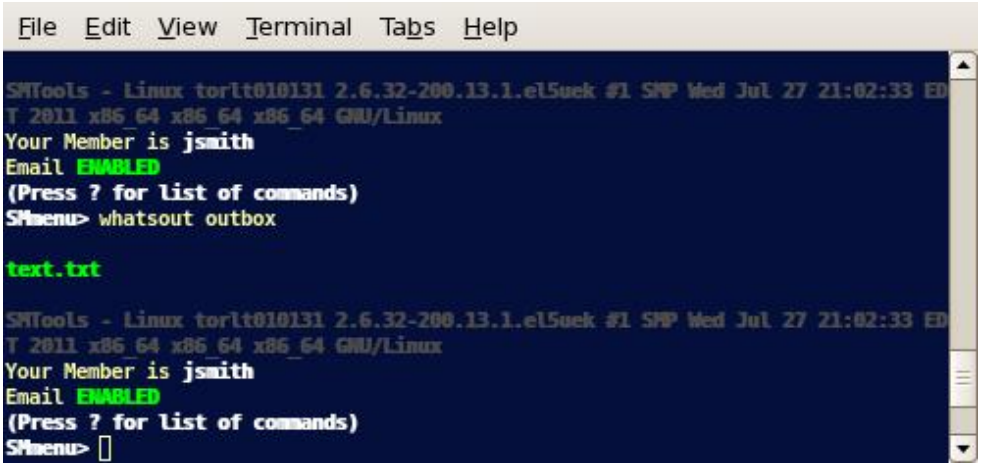
preparearchive {MemberName1,MemberName2... OR @ for all Memeber Keys}

The specially formed Archive File is created under $SM_OUTDIR. The following example demonstrates the typical workflow of creating and sending confidential message:

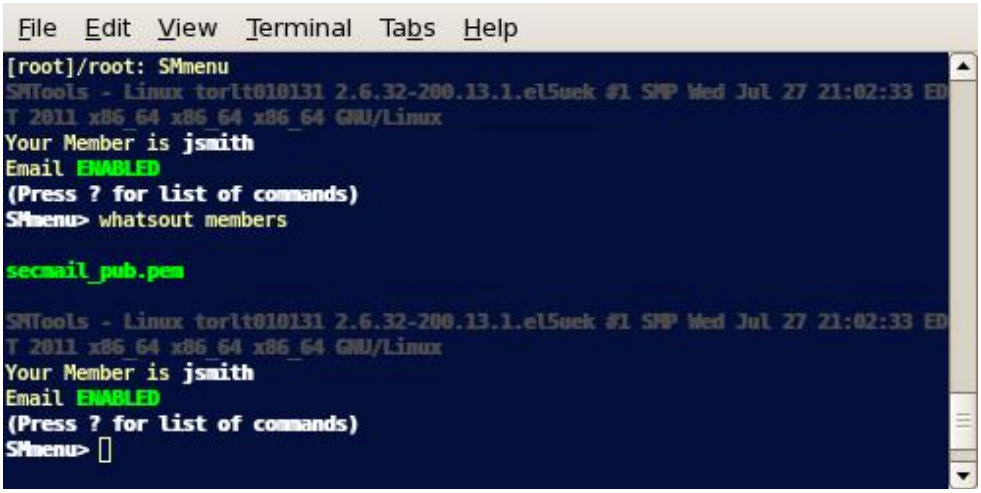
1. Edit your confidential message and save it into **$SM_OUTDIR**/outbox folder.
2. Obtain the Public Key of the target Member and save it into **$SM_OUTDIR**/members folder.
3. Invoke **SMmenu** and go through steps as in following pictures:


File Edit View Terminal Tabs Help
SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 EDT 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu> whatsout
members outbox
SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 EDT 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu>

^ The command **whatsout** shows the content of **$SM_OUTDIR** directory


File Edit View Terminal Tabs Help
SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 EDT 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu> whatsout outbox
text.txt
SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 EDT 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu>

^The **whatsout outbox** shows content of outbox directory – your message you created.

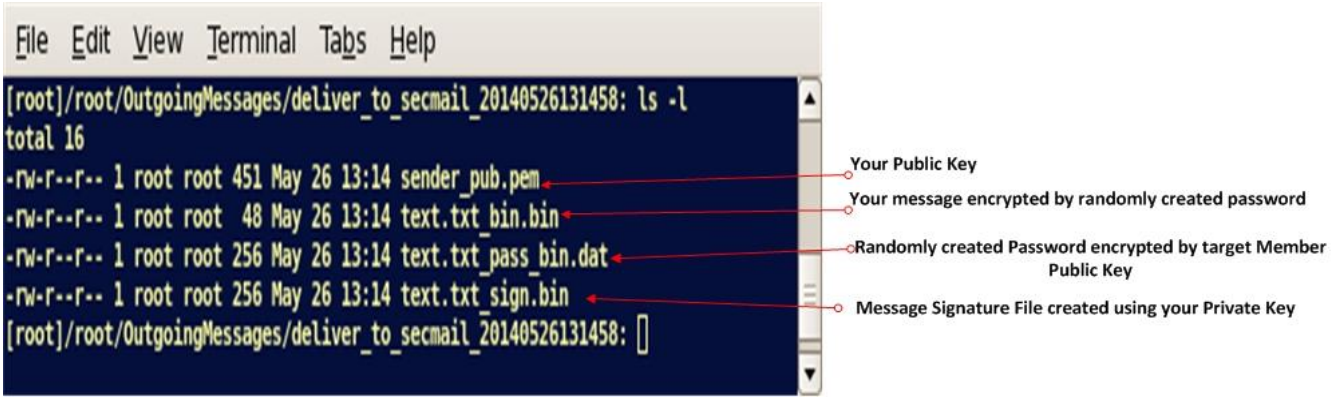

File Edit View Terminal Tabs Help
[root]/root: SMmenu
SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 EDT 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu> whatsout members
secmail_pub.pem
SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 EDT 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu>

^ The whatsout members shows the **Publec Keys** of the target Members (**secmail** in our case).

```
File  Edit  View  Terminal  Tabs  Help
(Press ? for list of commands)
SMmenu> whatsout members

secmail_pub.pem

SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 ED
T 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu> whatsout outbox

text.txt

SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 ED
T 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu> preparearchive secmail
Executing: SMwriter -d secmail

deliver_to_secmail_20140526131458.tar.bz2 has been created.

SMTools - Linux torlt010131 2.6.32-200.13.1.el5uek #1 SMP Wed Jul 27 21:02:33 ED
T 2011 x86_64 x86_64 x86_64 GNU/Linux
Your Member is jsmith
Email ENABLED
(Press ? for list of commands)
SMmenu> sendarchieve
```

^ The preparearchive command creates archive named **deliver_to_<MemberName>_<TimeStamp>.tar.bz2**

The content of the archive is as follow:


File Edit View Terminal Tabs Help
[root]/root/OutgoingMessages/deliver_to_secmail_20140526131458: ls -l
total 16
-rw-r--r-- 1 root root 451 May 26 13:14 sender_pub.pem
-rw-r--r-- 1 root root 48 May 26 13:14 text.txt_bin.bin
-rw-r--r-- 1 root root 256 May 26 13:14 text.txt_pass_bin.dat
-rw-r--r-- 1 root root 256 May 26 13:14 text.txt_sign.bin
[root]/root/OutgoingMessages/deliver_to_secmail_20140526131458:
Your Public Key
Your message encrypted by randomly created password
Randomly created Password encrypted by target Member Public Key
Message Signature File created using your Private Key

The **sendarchive** command will send the Archive to the edelivery@internetsecmail.com mailbox and the **InternetSecMail** Server will fetch this message and redirect the attached Archive to the email address of "secmail" **Member**.

Upon receiving, the "secmail" **Member** will save the attached Archive into **$SM_INDIR** incoming messages folder and open it by **archivein deliver_to_secmail_20140526131458.tar.bz2** command.

prepareandsend

The **prepareandsend** command is a shortcut to **preparearchive** and **sendarchive** commands which are executed in this case in a chain.

SMmenu general notes

1. The **SMmenu** is based on GNU Readline library that provides line editing and commands history capabilities. It allows users to move the text cursor, search the command history and use tab command completion.
   To move to previous/next command in History Buffer use UP and DOWN arrays.
   To complete command you started to type use TAB.
2. If the **SMmenu** needs to send the email to edelivery@internetsecmail.com, the User is assumed to be registered in **InternetSecMail** Server. If during the command processing the **InternetSecMail** Server detects that the User is not registered OR the Member is not valid, the request will be ignored by the Server Side.

SMreader and SMwriter programs

If you want, you can activate **SMreader** and **SMwriter** programs from the command line and see what the available run time options are. You also can refer to the source code for reference and better understanding of the process.